6560-50-P

ENVIRONMENTAL PROTECTION AGENCY

[FRL-10299-01-OMS]

Privacy Act of 1974; System of Records

AGENCY: Office of Mission Support (OMS), Environmental Protection Agency (EPA).

ACTION: Notice of a new system of records.

SUMMARY: The U.S. Environmental Protection Agency's (EPA) Office of Mission Support (OMS) is giving notice that it proposes to create a new system of records pursuant to the provisions of the Privacy Act of 1974. EPA is creating the Enterprise Physical Access Control System (ePACS) to collect and maintain employee and contractor information that is used to determine suitability for physical access to EPA-managed facilities and certain restricted areas within these facilities.

DATES: Persons wishing to comment on this system of records notice must do so by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE ***FEDERAL REGISTER***]. Routine uses; for this new system of records will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE ***FEDERAL REGISTER***].

ADDRESSES: Submit your comments, identified by Docket ID No. EPA-HQ-OMS-2022-0847, by one of the following methods:

Federal eRulemaking Portal: https://www.regulations.gov. Follow the online instructions for submitting comments.

Email: docket_oms@epa.gov. Include the Docket ID number in the subject line of the message.

Fax: (202) 566-1752.

Mail: OMS Docket, Environmental Protection Agency, Mail Code: 2822T, 1200 Pennsylvania Ave., NW, Washington, D.C. 20460.

Hand Delivery: OMS Docket, EPA/DC, WJC West Building, Room 3334, 1301 Constitution Ave., NW, Washington, D.C. 20460. Such deliveries are only accepted during the Docket's normal hours of operation, and special arrangements should be made for deliveries of boxed information.

Instructions: Direct your comments to Docket ID No. EPA-HQ-OMS-2022-0847. The EPA's policy is that all comments received will be included in the public docket without change and may be made available online at https://www.regulations.gov, including any personal information provided, unless the comment includes information claimed to be Controlled Unclassified Information (CUI) or other information for which disclosure is restricted by statute. Do not submit information that you consider to be CUI or otherwise protected through https://www.regulations.gov. The https://www.regulations.gov website is an "anonymous access" system for the EPA, which means the EPA will not know your identity or contact information. If you submit an electronic comment, the EPA recommends that you include your name and other contact information in the body of your comment. If the EPA cannot read your comment due to technical difficulties and cannot contact you for clarification, the EPA may not be able to consider your comment. If you send an e-mail comment directly to the EPA without going through https://www.regulations.gov, your e-mail address will be automatically captured and included as part of the comment that is placed in the public docket and made available on the internet. Electronic files should avoid the use of special characters, any form of encryption, and be free of any defects or viruses. For additional information about the EPA public docket, visit the EPA Docket Center homepage at https://www.epa.gov/dockets.

Docket: All documents in the docket are listed in the https://www.regulations.gov index. Although listed in the index, some information is not publicly available**,** e.g., CUI or other information for which disclosure is restricted by statute. Certain other material, such as copyrighted material, will be publicly available only in hard copy. Publicly available docket materials are available either electronically in https://www.regulations.gov or in hard copy at the

OMS Docket, EPA/DC, WJC West Building, Room 3334, 1301 Constitution Ave., NW, Washington, D.C. 20460. The Public Reading Room is normally open from 8:30 a.m. to 4:30 p.m., Monday through Friday excluding legal holidays. The telephone number for the Public Reading Room is (202) 566-1744, and the telephone number for the OMS Docket is (202) 566-1752. Further information about EPA Docket Center services and current operating status is available at https://www.epa.gov/dockets.

FOR FURTHER INFORMATION CONTACT: James Cunningham, Information Technology (IT) Project Manager, Office of Mission Support, Environmental Protection Agency, 1301 Constitution Ave, NW, Washington, D.C. 20460, *cunningham.james@epa.gov*.

Jackie Brown, Information System Security Officer, Office of Mission Support, Environmental Protection Agency, 1301 Constitution Ave, NW, Washington, D.C. 20460, *brown.jackie@epa.gov*.

SUPPLEMENTARY INFORMATION: Enterprise Physical Access Control System (ePACS) comprises non-traditional IT hardware such as Personal Identity Verification (PIV) card readers, control panels, closed circuit video cameras, building intrusion detection sensors, alarm keypads, and emergency door buttons that are tightly integrated into one ePACS system that is centrally managed in a virtual server environment. An employee or contractor must register their PIV card with ePACS. During the registration process, the following information is collected and stored in an ePACS centralized database: first name, last name, PIV card serial number, image, expiration date, affiliation (employee or contractor), and organization. Specific access clearances are then granted to a PIV card credential which allows access to EPA buildings, doors, rooms, elevators, and other physical access points. Information collected each time the PIV card credential is used is stored in the ePACS centralized database. This information assists EPA in monitoring its facilities, buildings, and other physical access points to ensure that only authorized personnel gain entry.

EPA is developing ePACS to comply with Homeland Security Presidential Directive-12: Policy for a Common Identification Standard for Federal Employees and Contractors (HSPD-12), and with the Office of Management and Budget (OMB) Memorandum M-11-11 Continued Implementation of HSPD-12. HSPD-12 mandates a government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors. M-11-11 requires use of a PIV credential as the common means of authentication for access to Federally-controlled facilities, networks, and information systems. To allow physical entry to EPA-controlled facilities and logical access to EPA information systems, ePACS uses PIV smartcard credentials issued to EPA employees and contractors. A PIV smartcard links an individual's identity to an identification credential that enables that person to gain physical access to federally-controlled buildings and logical access to information systems.

SYSTEM NAME AND NUMBER: Enterprise Physical Access Control System (ePACS), EPA-99.

SECURITY CLASSIFICATION: *Unclassified.*

SYSTEM LOCATION: The system will be managed by the Office of Mission Support, Environmental Protection Agency, 1301 Constitution Ave. NW, Washington, D.C. 20460. Electronically stored information is hosted at the EPA National Computer Center (NCC), 109 TW Alexander Drive, Research Triangle Park, Durham, NC 27711.

SYSTEM MANAGER(S): Alexandria DeLaCruz-Matthews, Program Manager, Office of Mission Support, Environmental Protection Agency, 1301 Constitution Ave, NW, Washington, D.C. 20460, *delacruz-matthews.alexandria@epa.gov*.

James Cunningham, IT Project Manager, Office of Mission Support, Environmental Protection Agency, 1301 Constitution Ave, NW, Washington, D.C. 20460, *cunningham.james@epa.gov*.

Jackie Brown, Information System Security Officer, Office of Mission Support, Environmental Protection Agency, 1301 Constitution Ave, NW, Washington, D.C. 20460, *brown.jackie@epa.gov*.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Government Organization and Employees, 5 U.S.C. 301; Management of buildings by Administrator of General Services, 40 U.S.C. 582; Lease agreements, 40 U.S.C. 585; Public Buildings under the control of Administrator of General Services, 40 U.S.C. 3101; Agency Chief Information Officer, 40 U.S.C. 11315; Federal Information Security Management Act of 2002, 44 U.S.C. 3501; 44 U.S.C. 3505, 44 U.S.C. 3506, 44 U.S.C. 3541; E-Government Act of 2002, 44 U.S.C. 101, Chapter 35; Federal Information Processing Standards Publication (FIPS) 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors, and HSPD-12.

PURPOSE(S) OF THE SYSTEM: The Agency will use the ePACS system to collect and maintain information required for and related to authorized physical access to all EPA-managed facilities and restricted areas within these facilities across the United States.

Collection and maintenance of this information will help to:

1. Ensure the safety and security of Federal facilities, systems, and information, and of facility occupants and users.
2. Provide for interoperability between systems and locations to individuals entering EPA facilities.
3. Ensure that all personnel (employees and contractors) entering EPA buildings have proper credentials and to protect against unauthorized access. The information will also provide an audit trail for investigations, if needed.
4. Allow logical access to Federal information systems, networks, and resources on a government-wide basis.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: EPA employees, contractor employees, interns, and volunteers that have valid credentials programmed for specific access points.

CATEGORIES OF RECORDS IN THE SYSTEM: Full name, photographs, surveillance video recordings and camera images, Full Cardholder Unique Identifier (CHUID), credential ID, PIV card number, Public Key Infrastructure (PKI) certificate—(X509), Card Authentication Key (CAK) certificate, person classification, badge expiration date, card state, User Principal Name (UPN), Federal Agency Smart Card Number (FASC-N), and Globally Unique Identifier (GUID).

RECORD SOURCE CATEGORIES: ePACS obtains information from employees, contractor employees, interns, and volunteers using their EPA PIV credential. This information is stored in a secure ePACS database and updated when the PIV credential is used at an access point. In addition, ePACS collects information from video cameras and video recording devices located at and within EPA facilities in the United States.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: The routine uses below are both related to and compatible with the original purpose for which the information was collected. The following general routine uses apply to this system (86 FR 62527): A, B, C, D, E, F, G, H, I, J, K, L, and M

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are stored on secure servers within the ePACS Master and Satellite Application Databases and can be accessed only by authorized users over EPA secure intranet using encryption software. These records are maintained electronically on computer storage devices located at the U.S. EPA National Computer Center, 109 T.W. Alexander Drive, Research Triangle Park, NC 27711.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Authorized user login/password credentials and administrative privileges are required to access the ePACS software application. ePACS records can only be accessed when logged in to the ePACS

application that pulls these records from the ePACS database. Records may be retrieved by first name, last name, full name, email address, FACSN, or Object ID Number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are retained and disposed of in accordance with applicable NARA retention schedules as well as EPA records schedules 089, 1008, and 1012.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: PII is safeguarded and protected in conformance with all Federal statutes and OMB requirements. Security controls used to protect personal sensitive data in ePACS are commensurate with those required for an information system rated MODERATE for confidentiality, integrity, and availability, as prescribed in National Institute of Standards and Technology (NIST) Special Publication, 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5.

1. Administrative Safeguards: Only authorized users are allowed access to ePACS. Each authorized user must complete a background investigation with favorable results, must be assigned to the appropriate security group, acknowledge agency rules of behavior, and complete annual privacy and security training. In addition, personnel are instructed to lock their computers when they leave their desks.

2. Technical Safeguards: All ePACS user access is limited by role-based restrictions. In addition, ePACS operators are required to enter a valid username and password to gain access to the system. Individuals granted access privileges are screened for proper credentials and added to the appropriate Microsoft Windows security group based on their Local Area Network account. EPA maintains an audit log trail for ePACS, which accounts for all instances of users accessing the system. EPA reviews audit logs periodically to identify any unauthorized access.

3. Physical Safeguards: All ePACS records are stored on database servers located in secure, access-controlled buildings. ePACS database and application servers are in access-controlled rooms that require PIV credentials for access. Only authorized users are allowed access to administrative accounts for ePACS application and database servers.

RECORD ACCESS PROCEDURES: All requests for access to personal records should cite the Privacy Act of 1974 and reference the type of request being made (i.e., access). Requests must include: (1) the name and signature of the individual making the request; (2) the name of the Privacy Act system of records to which the request relates; (3) a statement whether a personal inspection of the records or a copy of them by mail is desired; and (4) proof of identity. A full description of EPA's Privacy Act procedures for requesting access to records is included in EPA's Privacy Act regulations at 40 CFR part 16.

CONTESTING RECORD PROCEDURES: Requests for correction or amendment must include: (1) the name and signature of the individual making the request; (2) the name of the Privacy Act system of records to which the request relates; (3) a description of the information sought to be corrected or amended and the specific reasons for the correction or amendment; and (4) proof of identity. A full description of EPA's Privacy Act procedures for the correction or amendment of a record is included in EPA's Privacy Act regulations at 40 CFR part 16.

NOTIFICATION PROCEDURES: Individuals who wish to be informed whether a Privacy Act system of records maintained by EPA contains any record pertaining to them, should make a written request to the EPA, Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW, Washington, D.C. 20460, or by email at: privacy@epa.gov. A full description of EPA's Privacy Act procedures is included in EPA's Privacy Act regulations at 40 CFR part 16.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: None.

Vaughn Noga,
Senior Agency Official for Privacy.
[FR Doc. 2022-26903 Filed: 12/9/2022 8:45 am; Publication Date: 12/12/2022]